SOME EXPERIMENTS ON BATEMAN-HORN

IGOR RIVIN

Abstract. We describe some studies related to the frequency of prime values of integer polynomials.

1. Introduction

The Bateman-Horn conjecture (see [1]) states that given m irreducible polynomials $f_1, \ldots, f_m$ with integer coefficients, then the number of positive integers $k \leq x$ such that $f_i(k)$ is prime[1] for every $1 \leq i \leq m$ is asymptotic to

$$\frac{C}{D} \int_2^x \frac{dt}{\log^m t},$$

where D is the product of the degrees of the f_i, while

$$C(f) = \prod_p \frac{1 - n_p(f)/p}{1 - 1/p},$$

where $n_p(f)$ is the number of solutions of $f(x) = 0 \mod p$, where $f(x) = f_1 \cdots f_m$.

In this note, we look at the simplest case where $m = 1$, and study the behavior of the coefficient $C(f)$, where f is a random monic polynomial[2] in $\mathbb{Z}[x]$. Our model of a random polynomial is one where all the coefficients (except the leading one, which is always equal to 1) are uniformly chosen from the interval $[-N, N]$, where N is typically equal to 1000. Further, we approximate the constant $C(f)$ by taking the products over the first several primes (first 3000 primes in the experiment below). Now, there is also a finite probability that $C(f) = 0$ -

Date: September 1, 2015.

1991 *Mathematics Subject Classification.* 11P32, 11N37.

Key words and phrases. primes, polynomials, Bateman-Horn.

The author would like to thank the MathOverflow community for its support, and in particular, the user **joro** who asked the question which led to this note. The author would like to thank Keith Conrad for valuable suggestions.

[1]We allow our primes to be negative.

[2]Such a polynomial is almost surely irreducible, though in the experiments we throw away the few exceptional cases.

this would be true if the values of f are *always* divisible by p, for some prime p - obviously the most likely such prime is 2, so it makes sense to look at those f which don't always vanish mod p for any p (or, at least, any p we look at).[3]

Now, what do we look at?

- What is the mean value of $C(f)$ over our sample space? (whether all irreducible f or those f satisfying the Bunyakovsky condition?
- How are the values of $C(f)$ distributed (here, it only makes sense to look at those f satisfying the Bunyakovsky condition).
- What are the extremal values of C, and what property of the polynomials involved is responsible? (we have not studied this yet).

It should be noted that in the "orthogonal" direction (where we have a number of *linear* polynomials, which corresponds to the prime k-tuple conjecture), some statistical results were obtained by P. X. Gallagher [2] and E. Kowalski [3].

2. Some experimental observations

I looked at polynomials of degrees 2 through 6. Here are the means:

degree	mean	Bunyakovsky mean	Bunyakovsky log mean
2	1.00329	1.33525	0.0847562
3	1.00714	1.38343	0.129013
4	0.971798	1.35929	0.124901
5	1.00044	1.38399	0.132433
6	1.02139	1.40398	0.155772
7	1.02448	1.41654	0.166858
8	1.00884	1.36817	0.120447

It does not seem surprising that the mean of all the irreducible polynomials is very close to 1. However, I am unaware of any proof of this. Here is a somewhat relevant fact:

Lemma 2.1. *For each $f \in \mathbb{F}_p[x]$ let $n(f)$ be the number of zeros of f counted* without *multiplicity. Then, the mean value of $n(f)$ over all of $\mathbb{F}_p[x]$ is* 1.

Proof. Consider the variety V defined over $\mathbb{F}_p$ by

$$X^n + \sum_{i=0}^{n-1} Y_i X^i = 0.$$

[3]This is the so-called Bunyakovsky condition.

The statement of the Lemma is equivalent to asserting that there are p^n $\mathbb{F}_p$-points on V. However, if we rewrite the equation of V as

$$X^n + \sum_{i=1}^{n-1} Y_i X^i = -Y_0,$$

it becomes obvious that V is nothing but the affine space $\mathbb{A}^n$, so the result follows. □

Now, in our experiment we sample uniformly from polynomials in $\mathbb{Z}[x]$ with coefficients bounded above by C and below by $-C$, then reduce modulo p. When C is much bigger than P our sample space will contain all of $\mathbb{F}_p$, but with somewhat uneven multiplicity. When C is much smaller than p, our sample space contains only a small sliver of $\mathbb{F}_p$, so we are asserting that the $\mathbb{F}_p$ points of V are very well equidistributed. If we average over primes, such a result is true.

Lemma 2.2. *Let $f \in \mathbb{Z}[x]$ be irreducible over $\mathbb{Q}$. Then,*

$$\lim_{x\to\infty} \frac{\sum_{p\le x} n_p(f)}{\pi(x)} = 1,$$

where $n_p(f)$ is the number of zeros of f modulo p.

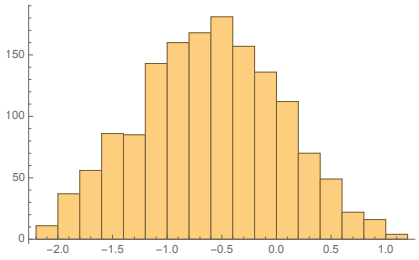
Proof. For each prime, let $s_f = \{d_1, \ldots, d_k\}$ be the set of degrees of irreducible factors of f modulo p. Chebotarev's theorem (see, e.g., [8]) says that the fraction of the primes for which a given s_f occurs is the same (asymptotically) as the fraction of the elements of the Galois group of f which have the cycle decomposition with lengths given by s_f. If f is irreducible, the Galois group of f is a transitive subgroup of S_n. The result now follows from Lemma 2.3 □

Lemma 2.3. *The average number of the fixed points of elements of a transitive permutation group equals* 1.

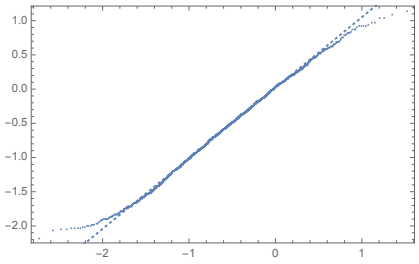
Proof. This follows from Burnside's lemma: for a group G acting on a set X, we have

$$|X/G| = \frac{1}{|G|} \sum_{g\in G} |X^g|,$$

where $|X/G|$ is the number of orbits of the G action, and $|X^g|$ is the number of fixed points of g. Since G acts transitively, the left hand side equals 1. □

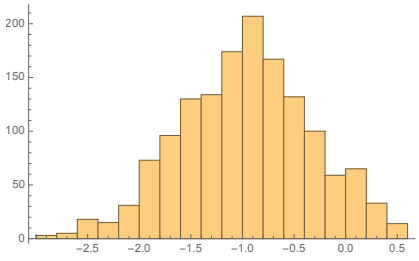


(A) Histogram of log $C(f)$

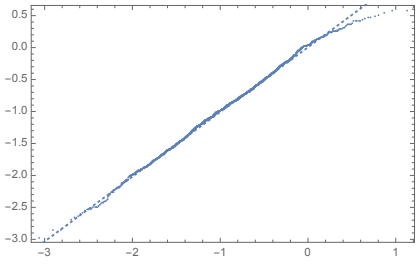


(B) quantile-quantile plot of log $C(f)$

FIGURE 1. Degree 2



(A) Histogram of log $C(f)$



(B) quantile-quantile plot of log $C(f)$

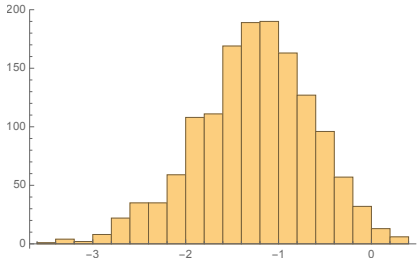
FIGURE 2. Degree 3

2.1. **The distribution.** As you may or may not be convinced by the charts below, the values of $C(f)$ for Bunyakovsky f (that is, an f which does not vanish identically modulo any prime p) seem to be log-normally distributed[4]. If true, this seems to indicate that the terms $1 - n_p/p$ are independent; the distributions for different p are not identical, but are the ones given by Chebotarev density. Now, independence for (very) small primes follows from the Chinese Remainder Theorem, but when the primes are large compared to the coefficients of our polynomials, that is far from clear.

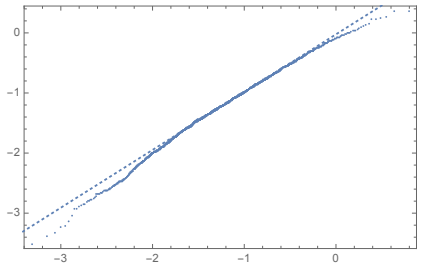
3. How prime-rich can a polynomial be?

As we have found (at least experimentally), the average value of $C(f)$ is 1, which means that a garden-variety monic (irreducible) polynomial of degree d, when given an argument of size around N, is about as likely to give a prime value as a number of size around N^d. We say that a polynomial is *prime-rich* if it is much more likely to give prime

[4]The graphs are of the Bateman-Horn quantity C/D, not of C.

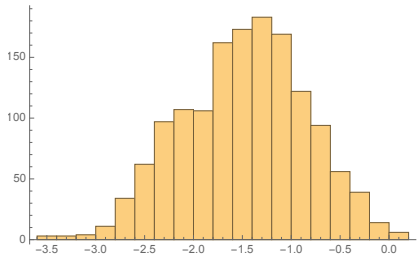


(A) Histogram of log $C(f)$

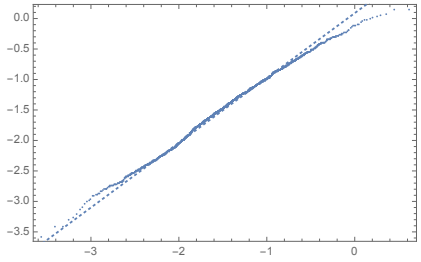


(B) quantile-quantile plot of log $C(f)$

FIGURE 3. Degree 4

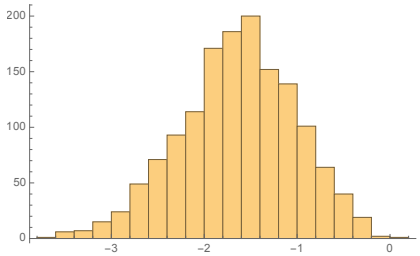


(A) Histogram of log $C(f)$

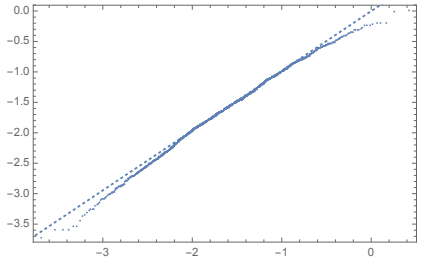


(B) quantile-quantile plot of log $C(f)$

FIGURE 4. Degree 5



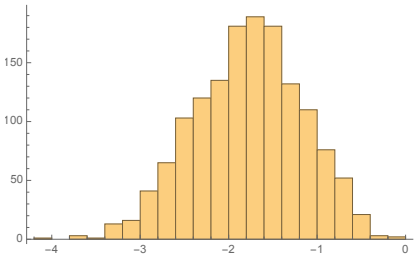
(A) Histogram of log $C(f)$



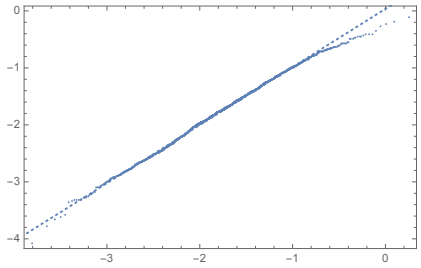
(B) quantile-quantile plot of log $C(f)$

FIGURE 5. Degree 6

values (which means that $C(f) > 1$). Of course, since just over a quarter of all polynomials fail the Bunyakovsky condition (the probability that a polynomial with content 1 in $\mathbb{Z}[x]$ gives even values always is around $1/4$, odd values always is $1/27$, and so on), the average Bunyakovsky polynomial is somewhat prime rich, but how well can we do?

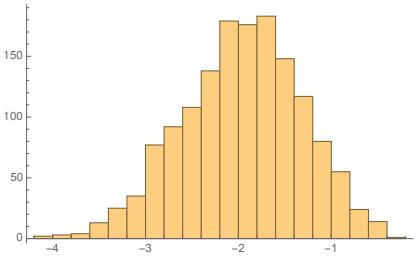


(A) Histogram of log $C(f)$

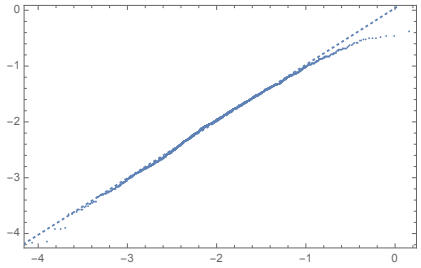


(B) quantile-quantile plot of log $C(f)$

FIGURE 6. Degree 7



(A) Histogram of log $C(f)$



(B) quantile-quantile plot of log $C(f)$

FIGURE 7. Degree 8

To find the answer, we computed 5000 random polynomials of coefficients bounded above by 5000 of each of the degrees $2, 3, 4, 5$, and found the ones most prime-rich. Below, we give the three richest for each of the degrees we computed, but not before asking:

Question 3.1. Is $C(f)$ bounded above (fixing degree)?

Of course, if the distribution of $C(f)$ is genuinely log-normal, then the answer is **NO.**

One place to look for an answer is in the proof that the product defining $C(f)$ actually converges. The proof (see [1]) uses Landau's Prime Ideal Theorem to observe that

$$\sum_{p<x} \frac{n_p(f)}{p} = \log\log x + A_f + o(1),$$

for *any* irreducible f (the constant A_f for $f(x) = x$ is the so-called Mertens-Meissel constant M). In turn, that implies that

$$\lim_{x\to\infty} \sum_{p<x} \frac{n_f(p) - 1}{p} = A_f - M,$$

which immediately implies that the product converges, and indicates that the size of $C(f)$ is controlled by the magic constant A_f, which does not seem to help that much.

Note that if we had some uniform estimate on the convergence speed of the Euler product, then the answer to the Question 3.1 is clearly negative: simply take a polynomial which has no roots for the first k primes (this is easy to do by Chinese remaindering) - the product of the first k terms of the defining product is going to be of order of $\log k$ (while the coefficients of the polynomial with given reductions mod p will be of order of e^k) - a uniform estimate on the remainder would finish the job. However, we are not aware of any such uniformity result (notice that it would be enough to have uniformity *on average*). If we remove the condition of being monic, then the obvious candidate (without Chinese remaindering) is the polynomial

$$P_{n,k}(x) = 1 + x^k \prod_{i=1}^{n} p_i.$$

A numerical experiment indicates that $C(P_{30,2}) \approx 9.5$. Modulo all of the above, one can ask a more detailed question:

Question 3.2. If we look at all $f \in \mathbb{Z}[x]$ of some fixed degree with coefficients bounded (in absolute value) by N, is it true that the maximal $C(f)$ is of order $\log\log N$?

One can look further, and look at whether more sophisticated methods of computing $C(f)$ than just multiplying out the beginning of the Euler products give us any clue. Such methods are described in a number of very nice papers by Nobushige Kurokawa[5] – [4, 7, 5, 6] - Kurokawa shows how to represent $C(f)$ as a product of Artin L-functions. Again, it is not clear how to leverage this to get a bound.

The other obvious question is:

Question 3.3. What do prime-rich polynomials have in common?

It is fairly clear (*assuming the truth of the Bateman-Horn conjecture*) that the constant term should be prime (or a product of large primes), and this is borne out by the results below.

Here are the winners (we give top three for each degree):

[5]The author would like to thank Keith Conrad for pointing these out to him.

$C(f)$	$f(x)$
6.3722	$x^2 - 2619x + 1291$
6.36569	$x^2 - 2717x - 1471$
6.23592	$x^2 + 2321x + 911$
5.51225	$x^3 + 3914x^2 - 3485x + 2773$
5.37671	$x^3 - 611x^2 - 424x - 2999$
5.35378	$x^3 + 707x^2 - 800x - 509$
6.19895	$x^4 - 1065x^3 + 409x^2 - 265x + 817$
5.74642	$x^4 + 254x^3 - 3125x^2 - 1204x - 2609$
5.65711	$x^4 + 4590x^3 - 4932x^2 + 2061x - 1289$
6.27693	$x^5 - 2127x^4 - 1190x^3 - 2317x^2 - 1499x - 2257$
6.15153	$x^5 - 4686x^4 + 2812x^3 - 4475x^2 - 1714x + 3389$
5.74885	$x^5 - 3738x^4 - 150x^3 - 4819x^2 - 2748x + 307$
6.86439	$x^6 + 2697x^5 + 3377x^4 + 2484x^3 - 2700x^2 + 1587x + 1831$
6.28748	$x^6 + 4705x^5 + 232x^4 - 3661x^3 + 3063x^2 - 820x - 3533$
6.12438	$x^6 + 1138x^5 - 2757x^4 - 4376x^3 + 954x^2 + 4060x - 2729$
5.72267	$x^7 + 1965x^6 + 2378x^5 - 2384x^4 - 1298x^3 - 600x^2 - 2610x - 1249$
5.62225	$x^7 - 4618x^6 + 4170x^5 + 4299x^4 + 1447x^3 + 4695x^2 + 2032x - 4387$
5.54845	$x^7 + 704x^6 - 2286x^5 - 1938x^4 - 462x^3 + 2470x^2 + 4241x - 2179$

References

[1] Paul T. Bateman and Roger A. Horn. A heuristic asymptotic formula concerning the distribution of prime numbers. *Mathematics of Computation*, 16(79):363–367, 1962.

[2] P. X. Gallagher. On the distribution of primes in short intervals. *Mathematika*, 23(1):4–9, 1976.

[3] Emmanuel Kowalski. Averages of Euler products, distribution of singular series and the ubiquity of Poisson distribution. *Acta Arith.*, 148(2):153–187, 2011.

[4] Nobushige Kurokawa. On some Euler products. II. *Proc. Japan Acad. Ser. A Math. Sci.*, 60(10):365–368, 1984.

[5] Nobushige Kurokawa. On the meromorphy of Euler products. I. *Proc. London Math. Soc. (3)*, 53(1):1–47, 1986.

[6] Nobushige Kurokawa. On the meromorphy of Euler products. II. *Proc. London Math. Soc. (3)*, 53(2):209–236, 1986.

[7] Nobushige Kurokawa. Special values of Euler products and Hardy-Littlewood constants. *Proc. Japan Acad. Ser. A Math. Sci.*, 62(1):25–28, 1986.

[8] Peter Stevenhagen and Hendrik Willem Lenstra. Chebotarëv and his density theorem. *The Mathematical Intelligencer*, 18(2):26–37, 1996.

University of St Andrews School of Mathematics and Statistics
E-mail address: igor.rivin@st-andrews.ac.uk